REMARKS

Claims 1-24 were pending and stand rejected. Claims 6, 14, and 21 have been cancelled. Claims 1-2, 5, 7, 9-10, 15-17, and 22-24 have been amended. Claims 1-5, 7-13, 15-20, and 22-24 are pending upon entry of this amendment.

On June 6, 2007, the Examiner left a voicemail for the undersigned attorney about an Information Disclosure Statement that was mailed by Applicant on August 17, 2006 and received by the Patent Office on August 22, 2006. The Examiner stated that he would consider the references cited therein and send Applicant an initialed Form 8A with the next office communication.

Claims 1-3, 5-11, 13-18, and 20-24 were rejected under 35 USC 103(a) as being unpatentable over Porras in view of Berthaud. Applicants respectfully traverse.

On July 18, 2007, the Examiner and the undersigned attorney had a telephone interview during which they discussed claim 1 as previously pending, Porras, and Berthaud. No agreement was reached. The substance of the interview is set forth herein.

As amended, claim 1 recites:

A network security system comprising:
- a first distributed software agent to collect a first stream of alerts from a first network security device having a first clock, each alert in the first stream representing an event detected by the first network security device and including a time of detection by the first network security device according to the first clock;
- a second distributed software agent to collect a second stream of alerts from a second network security device having a second clock, each alert in the second stream representing an event detected by the second network security device and including a time of detection by the second network security device according to the second clock; and
- a manager module in communication with the distributed software agents to:
  - receive the first and second stream of alerts;
  - identify a first alert in the first stream and a second alert in the second stream,
    - wherein the first alert includes an Internet Protocol (IP) address, and
    - wherein the second alert includes the IP address;

determine, based on the first alert and the second alert, whether the first clock and the second clock are synchronized; and

if the first clock and the second clock are not synchronized, synchronize the first clock and the second clock.

As described in the pending application, the claimed invention comprises a first software agent, a second software agent, and a manager module (¶¶12-15; FIG. 1). The manager module receives a first stream of alerts from a first network security device having a first clock and a second stream of alerts from a second network security device having a second clock (¶22). The manager module identifies a first alert in the first stream and a second alert in the second stream, wherein the first alert includes an Internet Protocol (IP) address, and wherein the second alert includes the IP address (¶¶23-24). The manager module determines, based on the first alert and the second alert, whether the first clock and the second clock are synchronized (¶26). If the first clock and the second clock are not synchronized, the manager module synchronizes the first clock and the second clock (¶26).

Applicants agree with the Examiner that Porras does not disclose, teach, or suggest synchronizing a first clock and a second clock using a common event. Also, while Porras mentions in passing the existence of a system clock (6:55-57), it does not disclose, teach, or suggest synchronization of clocks. It follows that Porras does not disclose, teach, or suggest the claimed element "determine, based on the first alert and the second alert, whether the first clock and the second clock are synchronized."

Berthaud does not remedy this deficiency. Berthaud discusses clock synchronization using a continuous conversion function (title). Each slave node in a communication network has its own local time base and exchanges timing information with a predefined master node whose time base is the master clock against which each node's local time base is to be synchronized (abstract). Time values measured at different slave nodes with different time bases are converted

into a unique time reference (master time) (5:1-3). Each slave maintains a mathematic conversion function of its local time into its master time (5:4-5). In order to get the parameters necessary to establish the conversion function, each slave regularly polls its master by exchanging synchronization messages (5:5-7).

Berthaud does not disclose, teach, or suggest the claimed element "determine, based on the first alert and the second alert, whether the first clock and the second clock are synchronized." The Examiner cited FIG. 2 and column 9, lines 35-60. These sections of Berthaud discuss how to compare the moments in time of occurrence of two events in different nodes of a network (9:43-45). The first event EV1 occurred in node A at local time T_{A1}, while the second event occurred in node E at local time T_{E2} (9:45-47). In order to compare the moments in time of occurrence of the events, it is necessary to refer to the same time base (9:47-49).

Claim 1 recites, in part, "wherein the first alert includes an Internet Protocol (IP) address, and wherein the second alert includes the IP address." The events in Berthaud (EV1 and EV2) do not include the same IP address as recited in claim 1. Thus, they cannot correspond to the claimed elements "first alert" and "second alert." Also, the events EV1 and EV2 are not used to determine whether the first clock (at node A) and the second clock (at node B) are synchronized as recited in claim 1. Instead, events EV1 and EV2 are merely converted to the same time base (at node C) so that their moments in time of occurrence can be compared (9:49-50; 10:12-22). It follows that Berthaud does not disclose, teach, or suggest the claimed element "determine, based on the first alert and the second alert, whether the first clock and the second clock are synchronized."

Thus, claim 1 (as amended) is patentable over Porras and Berthaud, both individually and in combination. Independent claims 9, 16, and 23 (as amended) recite similar language and are also patentable over Porras and Berthaud, both individually and in combination, for at least the same reasons.

Claims 4, 12, and 19 were rejected under 35 USC 103(a) as being unpatentable over Porras in view of Berthaud further in view of Apel. Applicants respectfully traverse. For the record, Applicants also traverse the Examiner's assertions regarding the disclosure of Apel and regarding the motivation to combine Porras and Berthaud and Apel.

The claims not specifically mentioned above depend from claims 1, 9, 16, or 23 (directly or indirectly), which were shown to be patentable over Porras in view of Berthaud. In addition, these claims recite other features not included in claims 1, 9, 16, or 23. Thus, these claims are patentable over Porras in view of Berthaud, for at least the reasons discussed above, as well as for the elements that they individually recite.

Applicants respectfully submit that the pending claims are allowable over the cited art of record and request that the Examiner allow this case. The Examiner is invited to contact the undersigned in order to advance the prosecution of this application.

Respectfully submitted,
HUGH S. NJEMANZE

Dated: July 18, 2007

By: /Sabra-Anne R. Truesdale/

Sabra-Anne R. Truesdale
Reg. No. 55,687
Fenwick & West LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041
Tel.: (650) 335-7187
Fax.: (650) 938-5200